IN THE CLAIMS

Please amend the claims as follows:

1. (currently amended) A computer-readable medium having a computer program product for performing virus detection on a file within a computer system, said computer-readable medium comprising:

computer program code for categorizing a plurality of virus signatures into a respective one of a plurality of anti-virus sets according to their characteristic, wherein each of said anti-virus sets contains virus signatures sharing at least one common characteristic;

computer program code for associating an executing agent with a subset of said plurality of anti-virus sets, wherein said executing agent is associated with a target file; and

computer program code for, in response to said target file being opened by said associated executing agent, scanning contents of said target file for viruses by applying virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

2. (previously presented) The computer-readable medium of claim 1, wherein said target file being opened by said associated executing agent is performed by an operating system.

3. (previously presented) The computer-readable medium of claim 1, wherein said computer-readable medium further includes computer program code for defining a rule to preclude scanning of said target file.

4. (previously presented) The computer-readable medium of claim 3, wherein said computer-readable medium further includes computer program code for, in response to said rule to preclude scanning of said target file, allowing said target file to execute without scanning said target file for viruses.

5. (previously presented) The computer-readable medium of claim 1, wherein said computer-readable medium further includes computer program code for marking said target file has been scanned and allowing said target file to execute in response to a determination that contents of said target file do not match any virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

6. (previously presented) The computer-readable medium of claim 1, wherein said computer-readable medium further includes computer program code for quarantining said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

7. (previously presented) The computer-readable medium of claim 1, wherein said computer-readable medium further includes computer program code for deleting said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

8. (previously presented) The computer-readable medium of claim 1, wherein said computer-readable medium further includes computer program code for periodically scanning said target file associated with said executing agent.

9. (previously presented) The computer-readable medium of claim 1, wherein said computer-readable medium further includes:

computer program code for arranging said plurality of anti-virus sets into a hierarchical structure having first and second levels, wherein said first level includes a

first anti-virus set containing virus signatures that are mutually applicable to a plurality of executing agents, wherein said second level includes a second anti-virus set containing virus signatures that are exclusively applicable to a subset of said plurality of executing agents.

10. (previously presented) The computer-readable medium of claim 1, wherein said computer-readable medium further includes:

computer program code for arranging said plurality of anti-virus sets into a hierarchical structure having a first level, a second level, and a third level, wherein first level includes a first anti-virus set containing virus signatures that are mutually applicable to a plurality of executing agents, wherein said second level includes a second anti-virus set containing virus signatures which are mutually applicable to a subset of said plurality of executing agents, wherein said third level includes a third anti-virus set containing virus signatures that are exclusively applicable to one of said subset of said plurality of executing agents.

11-29. canceled.

30. (previously presented) A method for performing virus detection on a file within a computer system, said method comprising:

categorizing a plurality of virus signatures into a respective one of a plurality of anti-virus sets according to their characteristic, wherein each of said anti-virus sets contains virus signatures sharing at least one common characteristic;

associating an executing agent with a subset of said plurality of anti-virus sets, wherein said executing agent is associated with a target file; and

in response to said target file being opened by said associated executing agent, scanning contents of said target file for viruses by applying virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

31. (previously presented) The method of claim 30, wherein said target file being opened by said associated executing agent is performed by an operating system.

32. (previously presented) The method of claim 30, wherein said method further includes defining a rule to preclude scanning of said target file.

33. (previously presented) The method of claim 32, wherein said method further includes in response to said rule to preclude scanning of said target file, allowing said target file to execute without scanning said target file for viruses.

34. (previously presented) The method of claim 30, wherein said method further includes marking said target file has been scanned and allowing said target file to execute in response to a determination that contents of said target file do not match any virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

35. (previously presented) The method of claim 30, wherein said method further includes quarantining said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

36. (previously presented) The method of claim 30, wherein said method further includes deleting said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

37. (previously presented) The method of claim 30, wherein said method further includes periodically scanning said target file associated with said executing agent.

38. (previously presented) The method of claim 30, wherein said method further includes:

arranging said plurality of anti-virus sets into a hierarchical structure having first and second levels, wherein said first level includes a first anti-virus set containing virus signatures that are mutually applicable to a plurality of executing agents, wherein said second level includes a second anti-virus set containing virus signatures that are exclusively applicable to a subset of said plurality of executing agents.

39. (previously presented) The method of claim 30, wherein said method further includes:

arranging said plurality of anti-virus sets into a hierarchical structure having a first level, a second level, and a third level, wherein first level includes a first anti-virus set containing virus signatures that are mutually applicable to a plurality of executing agents, wherein said second level includes a second anti-virus set containing virus signatures which are mutually applicable to a subset of said plurality of executing agents, wherein said third level includes a third anti-virus set containing virus signatures that are exclusively applicable to one of said subset of said plurality of executing agents.